Fixed point semantics and partial recursion in Coq
Yves Bertot, Vladimir Komendantsky

To cite this version:

HAL Id: inria-00190975
https://inria.hal.science/inria-00190975v11
Submitted on 24 Jul 2008
Abstract
We propose to use the Knaster–Tarski least fixed point theorem as a basis to define recursive functions in the Calculus of Inductive Constructions. This widens the class of functions that can be modelled in type-theory based theorem proving tools to potentially non-terminating functions. This is only possible if we extend the logical framework by adding some axioms of classical logic. We claim that the extended framework makes it possible to reason about terminating or non-terminating computations and we show that extraction can also be extended to handle the new functions.

Categories and Subject Descriptors F.3.1 [Logics and Meanings of Programs]: Specifying and Verifying and Reasoning about Programs; F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic—Lambda Calculus and Related Systems

General Terms Verification

Keywords least fixed point semantics, non-terminating functions, the Knaster–Tarski theorem, automated theorem proving, program extraction

1. Introduction
For theoretical computer scientists, the Knaster–Tarski least fixed point theorem, as well as its application – the first fixed point theorem of Kleene [30], is a firm theoretical ground to assert the existence of objects defined by recursive equations. These objects can be inductive types or recursive functions as in [17, 16]. We consider the following generalised statement of the Knaster–Tarski theorem [1]:

Theorem 1 (Knaster–Tarski; complete p.o.). Given a monotonic function \( f \) on a chain-complete partial order, consider the following transfinite sequence \( \{ x_i \} \):

\[
\begin{align*}
  x_0 &= \bot \\
  x_{i+1} &= f(x_i) \\
  x_\beta &= \text{the least upper bound of the chain } \{ f(x_i) \}_{\alpha < \beta}
\end{align*}
\]

if \( \beta \) is a limit ordinal.

The function \( f \) has a least fixed point obtained by an iterative process on \( \{ x_i \} \) starting from \( x_0 \). Moreover, if \( f \) is continuous then the least fixed point is obtained in at most \( \omega \) iterations.

To use this theorem, one should be able to express that the domain of interest has the required completeness property and that the function being considered is continuous. If the goal is to define a partial recursive function then this requires using axioms of classical logic, and for this reason the step is seldom made in the user community of type-theory based theorem proving. However, adding classical logic axioms to the constructive logic of type theory can often be done safely to retain the consistency of the whole system.

In this paper, we work in classical logic to reason about potentially non-terminating recursive functions. No inconsistency is introduced in the process, because potentially non-terminating functions of type \( A \rightarrow B \) are actually modelled as functions of type \( A \rightarrow B_\bot \); the fact that a function may not terminate is recorded in its type, non-terminating computations are given the value \( \bot \) which is distinguished from all the regular values, and one can reason classically about the fact that a function terminates or not. This is obviously non-constructive but does not introduce any inconsistency.

One of the advantages of type-theory based theorem proving is that actual programs can be derived from formal models, with guarantees that these programs satisfy properties that are predicted in formally verified proofs. This derivation process, known as extraction [27, 19], performs a cleaning operation so that all parts of the formal models that correspond to compile-time verifications are removed. The extracted programs are often reasonably efficient. In this paper, we also show that extraction can accommodate the new class of potentially non-terminating functions.

When axioms are added to the logical framework, three cases may occur: first, the new axioms may make the system inconsistent; second, the new axioms may be used only in the part of the models that is cleaned away by the extraction process; third, the axioms may be used in the part that becomes included into the derived programs. There is no need to discuss the first case which should be avoided at all costs. In the second case, the extraction process still produces a consistent program, with the same guarantee of termination even if this guarantee relies on classical logic reasoning steps. In the third case, the added axiom needs to be linked to a computation process that implements the behaviour predicted by the axiom. We claim that this can be done safely if the Knaster–Tarski least fixed point theorem is given a sensible computational content.

Kleene’s least fixed point theorem can be used to justify the existence of recursive functions, because these functions can be described as the least fixed point of the functional that arises in their recursive equation. However, it is necessary to ensure that the function space has the properties of a complete partial order and that the functional is continuous. These facts can be motivated using a sim-
ple development of basic domain theory. With the help of the axiom of definite description, this theorem can be used to produce a function, which we shall call fixp, that takes as argument a continuous function and returns the least fixed point of this function. When the argument of fixp is a functional, the least fixed point is a recursive function, which can then be combined with other functions to build larger software models.

With respect to extraction, we also suggest a few improvements to the extraction process that should help making sure that fairly efficient code can be obtained automatically from the formal models studied inside our extension of the Calculus of Inductive Constructions.

The Knaster–Tarski least fixed point theorem guarantees two important properties of the function that is defined by the iterative process. The first property is that the obtained function satisfies the fixed point equation. The importance of fixed point equations is straightforward [11]. This fixed point equation is useful when we want to prove properties of the function, for instance, that under some conditions it is guaranteed to terminate. The second property is that the least fixed point is obtained in at most $\omega$ iterations. As a result, we can reason by induction on the length of computations, thus providing a poor man’s approximation of what is called fixed point induction in [26]. This possibility allows to prove properties of the function result when it exists, and can also be used to prove that under some conditions a function fails to terminate.

In this paper, we give an overview of our basic formalisation of domain theory. Then, we show how this theory can be used in the definition of simple recursive functions. We give examples with proofs about recursive functions. We discuss extraction and execution of the recursive programs that are obtained in this way. Future work and related work is reviewed at the end of the paper.

All the experiments described in this paper were done with Coq [13, 6] and can be found in the Internet from the first author’s web page [1].

2. Domain-Theoretic Constructions

Our domain-theoretic development, found at [1], comprises basic ideas of domain theory built on the notion of a preorder, that is a theory of (pointed) complete preorders as formalised by C. Paulin-Mohring [24]. In addition to the constructive complete preorders of Paulin-Mohring, we introduce flat complete preorders that we define making certain non-constructive steps which are to be specified below. Various libraries of domain theory already exist in several proof systems. Therefore we just invite the reader to grasp the basic constructions by reading our development since these constructions are quite standard for such a library.

In the present paper we abbreviate “pointed complete preorder” as “cpo”, following the convention in [26], and we systematically omit the word “pointed”. In Figure 1, we summarise some useful notation.

We define the following inductive type which is equivalent to the standard option type of Coq:

```
Inductive partial (A : Type) : Type :=
Def : A -> partial A | Undef : partial A.
```

The type partial is introduced in order to provide the hiding mechanism that would prevent the user of our library to encode, for instance, a classical proof for the halting problem but still permit unconstrained use of the standard option type of Coq. This hiding mechanism, which is just a side-effect of the continuity proofs, ensures that no value of the kind Def x is returned in the case Undef of a pattern-matching constructor. The abstraction of the type partial also guarantees the safety of optimisations suggested in Section 3 (The consistency of the system and the validity of the extraction process do not depend on this abstraction.)

```
ord

<table>
<thead>
<tr>
<th>cpo</th>
<th>preorder</th>
</tr>
</thead>
<tbody>
<tr>
<td>o</td>
<td>(pointed) complete preorder, cpo</td>
</tr>
<tr>
<td>m</td>
<td>preordered function space</td>
</tr>
<tr>
<td>≤</td>
<td>preordered monotonic function space</td>
</tr>
<tr>
<td>O</td>
<td>preordered continuous function space</td>
</tr>
<tr>
<td>C</td>
<td>function cpo</td>
</tr>
<tr>
<td>M</td>
<td>monotonic function cpo</td>
</tr>
<tr>
<td>natord</td>
<td>natural numbers ordered by ≤</td>
</tr>
<tr>
<td>chain O</td>
<td>(preordered) function application</td>
</tr>
<tr>
<td>≡</td>
<td>monotonic function composition</td>
</tr>
<tr>
<td>⊥</td>
<td>derived equality on the preorder O</td>
</tr>
</tbody>
</table>

```

**Figure 1.** Notation

The flat preorder on a type $A$ is defined by specifying a binary relation $\leq_{\text{flat}}$ on $A$ such that, for $x, y : A$, $x \leq_{\text{flat}} y$ iff $x = y$ or $x = Undef$. We denote this flat preorder by $\& A$.

Lifting of the flat preorder to a flat cpo requires a non-constructive definition for the lub function. Namely, using the excluded middle law of classical propositional logic we can prove $\leq_{\text{flat}} A$ being complete in a sense that, for each chain $c$ on $\& A$, there exists an $x$ such that $\forall n, c n \leq_{\text{flat}} A x$ and $\forall y, (\forall n, c n \leq_{\text{flat}} A y) \rightarrow x \leq_{\text{flat}} A y$, which proves the two laws for the required least upper bound function. Since we can prove that this least upper bound is unique, using the classical definite description axiom:

```
Axiom constructive_definite_description :
\forall A (P : A -> Prop), \exists x : A, P x \rightarrow \{ x : A | P x \}.
```

we obtain a $\Sigma$-type definition for the least upper bound of a chain $c$ on $A$ which contains two parts: an element $a$ of $\& A$ and the proof of $a$ being the least upper bound of $c$. In this way we obtain the function $\text{lub}_{\& A} : \text{chain} (\& A) \rightarrow \& A$ as the first projection of this $\Sigma$-type object. Thus we have a cpo structure on $\& A$; we denote it by $\& cpo A$.

The constructive definite description axiom is quite strong. However, it does not make the system inconsistent, assuming the predicative Set. By introducing this axiom the only thing one loses is the assurance that it will be possible to extract a sensible program form any proof. In Section 3 we show how the extraction mechanism can be instructed to extract correct programs from definitions made with our library.

The constructive definite description axiom is incompatible with variants of the Calculus of Constructions, where the Set sort is impredicative, due to the Chicli–Pottier–Simpson paradox [11] which was shown to hold for even a weaker version, the classical definite description axiom (in $\text{Prop}$ rather than $\text{Type}$), in the presence of classical logic. Therefore our development is restricted to the predicative Set which is, fortunately, default for Coq.

3. Kleene’s Fixed Point Theorem

The well-known fixed point theorem of Kleene, see [30], has a mild generalisation in the setting of complete preorders. Below we outline a formalised proof for this statement. Our proof follows the lines of the classical textbook proofs found in, e.g., [12, 26]. The fixed point functional defined for this proof can and will be used in this paper to define partial recursive functions and reason about them.

The construction of the fixed point functional is closely related to the one given in [26]. First, we define a function $\text{fixer}$ as follows (⊥ denotes the bottom element of the cpo $D$):

```
fixer : Σ (A : Type) (P : A -> Prop), \exists a : A, \forall x : A, P x \rightarrow \{ a : A | P a \}.
```

We obtain a $\Sigma$-type definition for the least upper bound of a chain $c$ on $A$ which contains two parts: an element $a$ of $\& A$ and the proof of $a$ being the least upper bound of $c$. In this way we obtain the function $\text{lub}_{\& A} : \text{chain} (\& A) \rightarrow \& A$ as the first projection of this $\Sigma$-type object. Thus we have a cpo structure on $\& A$; we denote it by $\& cpo A$.

```
4. Fixed Point Definitions of Partial Recursive Functions

To model partiality of a function \( f_0 \) with arguments of type \( A \) and values of type \( B \), first we define a recursive function \( f : A \rightarrow \text{cpo} B \) for which we ought to construct a continuous functional \( F \) of type

\[
(A \rightarrow \text{cpo} B) \rightarrow (A \rightarrow \text{cpo} B)
\]

such that \( f = F f \). A proof of such a functional \( F \) being continuous is usually non-trivial but considerably regular. For a proof, one might use the following intuition: The condition of continuity of \( F \) corresponds to the interpretation of “potential non-termination” according to which every expression containing a potentially non-terminating computation should fail to terminate if it actually uses the value returned by this computation and that computation fails to terminate. To use the value of a potentially non-terminating computation one needs to write a pattern-matching construct on this computation: the continuity condition will be satisfied if we ensure that the value \( \text{Undef} \) is returned in the case \( \text{Undef} \) of this matching construct.

For example, consider the minimisation functional \( \mu \) defined as follows: for all \( A \) : Type, \( f : A \rightarrow \text{nat} \rightarrow \text{nat} \), the value of \( \mu f \) is a function \( g : A \rightarrow \text{nat} \) such that \( g x \) is defined and has value \( y \) if and only if \( y \) is the least value for which \( f y = 0 \) holds. From this definition it follows that \( g x \) is undefined in case no least value \( y \) is found, that is \( \mu \) can be used to define partial functions.

Let \( A : \text{Type} \) and \( f : A \rightarrow \text{nat} \rightarrow \text{partial nat} \). First, we specify a functional \( f_{\text{mu}} \) as follows:

\[
\text{Definition } f_{\text{mu}} (\text{mu} : A \rightarrow \text{nat} \rightarrow \text{partial nat}) : A \rightarrow \text{nat} \rightarrow \text{partial nat} :=
\]

\[
\begin{align*}
\text{fun } x y & \Rightarrow \\
& \text{match } f x y \text{ with } \\
& \text{Undef } & \Rightarrow \text{Undef} \\
& \text{Def } 0 & \Rightarrow \text{Def } y \\
& \_ & \Rightarrow \text{mu } x (S y)
end.
\end{align*}
\]

Next, we demonstrate some proof ideas concerning this partial recursive function.

5. Certification of Functions

In \([35]\), Winskel describes fixed point induction as a technique for proving properties of least fixed points of continuous functions. This style of induction is restricted to certain predicates which are called refining in his work. The same notion also appears in HOLCF, see [39, 31], under the name of admissible predicates and the authors argue that it is important to provide strong automation facilities to manage the corresponding proofs of admissibility. Our work is less advanced than HOLCF – we do not provide automated admissibility proofs – still we provide basic techniques for proofs about recursive functions with flat target types.

In our setting, we want to prove properties of functions obtained using fixp and we have two tools at hand. The first tool is the lemma fixp_eq. The second tool is an omnipresent lemma that we employ to return a value of the least upper bound of a chain on a flat cpo:

\[
\text{Lemma lub_flat_cpo_witness : } \\
\forall (c : \text{chain } \& \text{cpo}), \exists n, c n = \text{lub } c.
\]

The above lemma can be used to prove that, for any input, the value of fixp \( f \) can also be computed by \( \text{iter } f n \) for some natural number \( n \):

\[
\text{Lemma fixp_flat_witness : } \\
\forall (A : B) : \text{Type}, (f : (A \rightarrow \text{cpo } B) \rightarrow (A \rightarrow \text{cpo } B)) \text{, } (x : A), \text{, } \exists n, \text{ fixp } f x = \text{iter } f n x.
\]

Proof:

intros A B f x.
Next, we extract a witness n using \( \text{lub}_{\text{flat cpo}} \text{witness} \) from the chain \( \text{iter } f \preceq x \) on \&cpo B; the witness equality (\( \text{iter } f \preceq x ) n = \text{lub } (\text{iter } f \preceq x ) \) is given the name Hn:

\[
\text{destruct } (\text{lub}_{\text{flat cpo}} \text{witness } (\text{iter } f \preceq x )) \text{ as } [n \text{ Hn}].
\]

We provide this n as the witness:

\[
\text{exists } n.
\]

and rewrite the goal with the witness equality:

\[
\text{rewrite } \text{Hn}.
\]

We arrive at the goal \( \text{fixp } f x = \text{lub } (\text{iter } f \preceq x ) \) which is proved by unfolding the structure of f:

\[
\text{case } f; \text{ intro } f'; \text{ case } f'; \text{ reflexivity}.
\]

Qed.

Thus the number n is an upper bound on the number of recursive calls that are needed to compute the value of \( f x \). Thanks to this theorem, one can reason by induction on n and simulate the fixed point induction of [H]. Notably, there is an additional match goal with step required before the rewrite step in some specific versions of Coq where the unification algorithm is not powerful enough to solve the given higher-order unification problem.

For instance, using \( \text{fixp}_{\text{flat witness}} \) we can conclude by simulating the fixed point induction with the following lemma which asserts that the function \text{perfect_sqrt} never terminates on inputs not being perfect squares.

**Lemma perfect_sqrt_Undef** :
\[
\forall x, (\forall y:\text{nat}, x \neq y^2) \rightarrow \text{perfect_sqrt } x = \text{Undef}.
\]

**Proof.**

\[
\text{intros } x Hx.; \text{ unfold perfect_sqrt, mu.}
\]

\[
\text{destruct } (\text{fixp}_{\text{flat witness}} x) \text{ as } [\text{cont}_{\mu} \text{nat abs } \text{minus } \text{y squared} 0 x y = \text{Undef}].
\]

\[
\text{rewrite } \text{Hn}.
\]

\[
\text{apply perfect_sqrt_Undef } \text{iter } \text{with } (1:=\text{Hx}).
\]

Qed.

For the proof, we extract a witness n and give the name Hn to the corresponding witness equality:

\[
\text{Hn: } \text{fixp } (\text{cont}_{\mu} \text{nat abs } \text{minus } \text{y squared} 0 x y = \text{Undef} ) 0 x = \text{Undef}
\]

then, after the rewrite step, we arrive at the goal

\[
\text{iter } (\text{cont}_{\mu} \text{nat abs } \text{minus } \text{y squared} 0 x y = \text{Undef} ) n 0 = \text{Undef}
\]

that is proved by a technical lemma we will explain shortly. In the proof of this lemma we refer to the two-argument version of \text{fixp}_{\text{flat witness}} (which can be proved either directly or by uncurrying followed by an application of the one-argument

**Lemma fixp_{flat witness}**: \[
\forall A B C (f : (A \rightarrow B \rightarrow \&\text{cpo } C) \rightarrow (A \rightarrow B \rightarrow \&\text{cpo } C)) x y, \exists n, \text{fixp } f x y = \text{iter } f n x y
\]

and then we refer to the following statement proved by induction on n:

**Lemma perfect_sqrt_Undef :**
\[
\forall n x y, (\forall z:\text{nat}, x \neq z \times z) \rightarrow \text{iter } (\text{mono } \mu \text{abs } x \times \text{minus } y \text{ squared} 0 x y = \text{Undef}
\]

**Proof.**

\[
\text{induction } n.
\]

Now we have to prove the inductive basis:

\[
\forall x y:\text{nat}, (\forall z:\text{nat}, x \neq z \times z) \rightarrow \text{iter } (\text{mono } \mu \text{abs } x \times \text{minus } y \text{ squared} 0 x y = \text{Undef}
\]

and the proof is easy:

\[
\text{reflexivity}.
\]

Next, we prove the inductive step:

\[
\forall x y:\text{nat}, (\forall z:\text{nat}, x \neq z \times z) \rightarrow \text{iter } (\text{mono } \mu \text{abs } x \times \text{minus } y \text{ squared} 0 x y = \text{Undef}
\]

which we do by case analysis:

\[
\text{simp; unfold fixp; simp.}
\]

\[
\text{intros } x y \text{Hxneq.}
\]

\[
\text{case_eq } (x - y \times y + (y \times y - x)).
\]

The first case, \( x \cdot y^2 + (y \cdot y \cdot x) = 0 \); we conclude by contradiction:

\[
\text{intro } \text{Heq0.}
\]

\[
\text{contradiction } (\text{Hxneq } y); \text{omega.}
\]

The second case, \( x \cdot y^2 + (y \cdot y \cdot x) = S \cdot n \circ 0 \); we conclude by the inductive hypothesis, that is \( \text{Hn:}
\]

\[
\text{intros } \text{Hx.}
\]

\[
\text{apply } (\text{Hx} \times (S \circ y) \circ \text{Hxneq}).
\]

Qed.

The third tool provided in our library is the following lemma that relates computations done with iter and values of a recursive function:

**Lemma iter_{Def}eq_{fixp}** :
\[
\forall A B C (f : (A \rightarrow B \rightarrow \&\text{cpo } C) \rightarrow (A \rightarrow B \rightarrow \&\text{cpo } C)) x n v,
\]

\[
\text{iter } f n x = \text{Def } v \Rightarrow \text{fixp } f x = \text{Def } v.
\]

Using this lemma, one can compute values of recursive functions, provided that none of these values is \text{Undef}. One simply needs to guess the right argument n that leads to a definite value of the form \text{Def } v which in this case is known to be the value of the recursive function for the corresponding argument. The problem is to decide whether a given number n is the right one. If the chosen value is too small, the value returned by the iterative process is the uninformative \text{Undef}.

For the sake of the example below we can prove the two-argument version \text{iter}_{Def}eq_{fixp} by uncurrying and then applying \text{iter}_{Def}eq_{fixp} (the alternative direct proof is easy):

**Lemma iter_{Def}eq_{fixp 2}** :
\[
\forall A B C (f : (A \rightarrow B \rightarrow \&\text{cpo } C) \rightarrow (A \rightarrow B \rightarrow \&\text{cpo } C)) x n v,
\]

\[
\text{iter } f n x = \text{Def } v \Rightarrow \text{fixp } f x = \text{Def } v.
\]

Now we can demonstrate a simulation of an iterative computation:

**Lemma compute_{perfect_sqrt 36}** : \text{perfect_sqrt 36 = Def } 6.

**Proof.**

\[
\text{unfold perfect_sqrt, mu.}
\]

\[
\text{apply iter_{Def}eq_{fixp 2} with } (n:=100); \text{reflexivity.}
\]

Qed.

The number 100 used in this example is only required to be an upper bound on the recursive calls enough to compute \text{perfect_sqrt 36} (in this case 7 would be enough). This approach may be used in reflexive tactics, for example, in a proof that involves computation of the value of a recursive function. One can try a fixed number of calls, and if a value of the form \text{Def } is returned, the proof can proceed, otherwise the tactic fails, which nevertheless does not signify the divergence of the recursive function.
6. Extraction to Functional Programming

Languages

The function perfects from Section 8 can be successfully extracted using the extraction mechanism provided by Coq. The extracted code exhibits the expected partial behaviour, that is it loops exactly on arguments which are not perfect squares. Below we show how this can be made possible.

Some of our lemmas rely on the Classical and ClassicalDescription extensions of the Coq libraries. These extensions add only two axioms to the logic of Coq, namely, the axiom of excluded middle, and the constructive definite description axiom: \( \forall A (P \land A \rightarrow \text{Prop}), (\exists x : A, P x) \rightarrow \{ x : A \mid P x \} \). The antecedent states that there exists a unique \( x \) satisfying the property \( P \) but it does not provide a method to construct \( x \). The consequent asserts that one can use this unique \( x \) as a constructive value. Using this axiom, one eliminates the distinction between constructive values and logically unique values. This of course disrespects the distinction between Set and logically unique values. This of course disrespects the distinction between Set and Prop that plays the central role during the extraction process of Coq.

The extraction mechanism relies on the assumption that, for every element of the form \( \{ x : A \mid P x \} \), there exists a constructive procedure for obtaining the \( x \)'s part. However, the axiom produces elements of that form without providing any constructive procedure. For example, the flatcpo type extracts to OCaml as:

```ocaml
let flatcpo = | O | P | lub = (Obj.magic (Obj.magic (Undef))); lub = (fun x -> projT1 (ExistT
[(match excluded_middle_informative with
| Left -> constructive_definite_description _
| Right -> Obj.magic Undef). _)]));
```

Obj.magic casts a value of any type into type Obj.t, which is convertible with any type, and is used, in this example, by the Coq extraction mechanism to represent implicit coercions. The fixp functional in OCaml, after systematic inlining of functions and erasing occurrences of Obj.magic, becomes:

```ocaml
let fixp d = fun n -> d lub (neter (((fun c -> c) n))
```

Thus one can see that, in OCaml, the lub of a flatcpo has essentially no computational content, and therefore fixp on a flat cpo does not compute the expected value. For this reason, the extraction mechanism expects the user to handwrite the procedure that returns the expected value wherever the axiom is used.

We propose the following solution to this problem. The constructive definite description axiom is only used in the definition of the function fixop, to transform the existential statement of Theorem 1 into a value that can be used in other functions. We can provide a handwritten constructive content for the function fixop, so that the logical value of this function is not used, and hence make sure that the definite description axiom is never used in the extracted code. We simply need to choose a constructive procedure for fixop that can be written in the target language of extraction and whose behaviour corresponds to the behaviour described in the Coq development.

We construct a function fix that computes the fixed point of functionals. This function should satisfy the following equality:

\[
\text{fix } (\text{fix } d \ f) = \text{fix } d \ f
\]

The introduced argument \( d \) corresponds to the cpo argument in Coq that is in most cases implicit there but explicit in OCaml. Changing the orientation of the equation seems enough to do the job:

```ocaml
let rec fix d f = f (fix d f)
```

However, this is not satisfactory in a call-by-value language, since this code directly attempts to compute fix \( d \ f \) again and enters a looping computation. Execution can be delayed as follows:

```ocaml
let fix d f = Obj.magic (Obj.magic (fixp (funcpo (funcpo flatcpo))))
```

The obtained function fix is the function we propose to attach to the function fixp for extraction purposes. The corresponding instruction to the Coq extraction mechanism is the following:

\[
\text{Extract Constant fixop} \Rightarrow \\
\text{"let rec fixd f x = f (fun y -> fixd f y) x in fix"}
\]

There is a leap of faith in this binding, which is as strong as the leap of faith one does when using extra axioms. In our current understanding of this extraction strategy, we can give a partial correctness result: when computation terminates and returns a first-order value, the result is still predicted by the Coq model.

The extracted OCaml code is for the function \( \text{mu} \) as shown in Figure 2. Occurrences of Obj.magic correspond to implicit coercions that appear in Coq.

For the rest of this section we assume that the argument \( d \) of fix is implicit.

**Theorem 3.** If the extracted code for fixop \( f \ a \) is some expression \( f' \ a' \), and the computation of fix \( f' \ a' \) terminates in the target language, then the expression fixop \( f \ a \) can be proved to terminate with the corresponding value in Coq.

**Proof.** Assume that the extraction process behaves correctly for expressions that do not contain fixop. We reason by induction on the number of steps in execution of fix \( f' \ a' \). When fix \( f' \ a' \) is being executed, the first steps lead to execution of \( f' \ (\text{fun } y \rightarrow \text{fix } f' y) \ a \), and the subsequent steps concern execution of \( a \) and \( f' \). Any execution of a fix expression occurring in \( f' \) or a uses less steps; hence, these executions behave as predicted by the corresponding fixop expression in the Coq model. Moreover, execution of \( (\text{fun } y \rightarrow \text{fix } f' y) \ e \) has the same behaviour as execution of fix \( f' \ e \). Together with the assumption that the extracted code in \( f' \) and \( a' \) outside of fix expressions behaves as expected, the latter consideration ensures the property.

In our model of recursive functions, the value Undef is only used for functions that are undefined because they fail to terminate (and hence Undef expresses divergence). We say that a Coq expression contains a spontaneous divergence if it contains an instance of Undef which is not encapsulated inside a pattern-matching construct on the type partial, or if it appears in any of the parts \( e \) and \( e2 \) of a pattern matching construct of the following shape:

\[
\text{match } e \text{ with Undef } \Rightarrow e1 \mid \text{Def } \Rightarrow e2 \text{ end}
\]
The functions we produce in Coq always satisfy the property
that they contain no spontaneous divergence. We can also assume
that programs extracted to OCaml or Haskell inherit the corre-
sponding property from the initial Coq functions. We will now
discuss optimisations that can be performed for this class of programs.

We have the following result:

**Theorem 4.** If an expression \( e \) contains no spontaneous divergence
then its value can never be the value \( \text{Undef} \).

**Proof.** One proves the statement by induction on the length of
execution of \( e \). The only sub-expressions that can produce the value
\( \text{Undef} \) are the \( \text{Undef} \) expressions that appear in the \( \text{Undef} \) branch
of a pattern-matching construct. In the pattern-matching construct,
the matched expression also has the property of containing no
spontaneous divergence and one can therefore use the induction
hypothesis.

We verified a formal Coq model of this proof in the context of
the Mini-ML language \([2]\) extended with a data-type representing
the type partial and the corresponding pattern-matching construct
\([2]\).

If values \( \text{Undef} \) can never be produced then the encapsulations
of expressions inside the constructor \( \text{Def} \) and the operations of
removing the constructor \( \text{Def} \) done by pattern-matching turn out to
be redundant. These, along with the occurrences of type partial, can
be recursively eliminated from the program since every instance of
\( \text{Def} \ e \) can be replaced with \( e \) and every instance of the construct

\[
\text{match } e \text{ with } \text{Undef} \Rightarrow e_1 \mid \text{Def } x \Rightarrow e_2
\]

can be replaced with let \( x = e \) in \( e_2 \). In what follows, we denote
by \( e \downarrow \) the result of this recursive elimination in \( e \).

**Theorem 5.** If \( e \) is an expression containing no spontaneous diver-
gence and the value of execution of \( e \) is \( v \) then the value of execution
of \( e \downarrow \) is \( v \downarrow \).

As in Theorem 4, the statement can be proved by induction on the
length of execution of \( e \). We actually prove a more general state-
ment which also includes the environments in which \( e \) and \( e \downarrow \) are
executed: we need to assume that the expression \( e \) is executed in an
environment \( \rho \) and the expression \( e \downarrow \) is executed in an environment
\( \rho \downarrow \), so that the value associated to each variable in \( \rho \downarrow \) is obtained
by applying the elimination to the corresponding value in \( \rho \).

For example, if the value of \( e \) is \( \text{Def} 3 \) then the value of \( e \downarrow \) is \( 3 \).
If \( e \) is \( \text{fun } x \rightarrow \text{Def} a \), and the current environment binds \( a \) with
\( \text{Def} 3 \) and \( b \) with \( 4 \), then the value of \( e \downarrow \) is the closure that can be written

\[
\text{fun } x \rightarrow \text{Def} a, (a, \text{Def} 3) : (b, 4)
\]

In this case, \( e \downarrow \) is \( \text{fun } x \rightarrow a \), the transformed environment binds \( a \)
with the value 3 and \( b \) with 4, and the result of the evaluation of \( e \downarrow \)
is

\[
\text{fun } x \rightarrow a, (a, 3) : (b, 4)
\]

**Proof.** Here we focus on the two most important cases:

1. If \( e \) has the form \( \text{Def} e_1 \) then \( e_1 \) also contains no spontaneous
divergence, and we can use the induction hypothesis on the
evaluation of \( e_1 \). Hence if \( v_1 \) is the value of \( e_1 \), the value of
\( e_1 \downarrow \) is \( v_1 \downarrow \). But in this case, we have \( e' = e_1 \downarrow \) and the value of
\( e \) is \( \text{Def} v_1 \downarrow \). However, we obviously have \( (\text{Def} v_1 \downarrow ) \downarrow = v_1 \downarrow \),
which justifies the result.

2. If \( e \) has the form

\[
\text{match } e_1 \text{ with } \text{Undef} \rightarrow \ldots \mid \text{Def } x \rightarrow e_2
\]

then \( e_1 \) is the expression

\[
(** \text{val } \mu : (\alpha 1 \rightarrow \text{nat} \rightarrow \text{nat}) \rightarrow \text{Obj} \text{.} \)
\]

let \( \mu f = \)

\[
\text{Obj} \text{.} \text{magic} \ (\text{Obj} \text{.} \text{magic} \ (\text{fixp} \ (\text{funcp} \ (\text{funcp} \ \text{flat} \text{.} \text{cpo})))))
\]

\[
\text{Obj} \text{.} \text{magic}
\]

\[
\text{Obj} \text{.} \text{magic} \ (\text{fun } x \ x0 \ x1 \rightarrow
\text{match } f x0 \ x1 \text{ with }
| \_ \rightarrow x1
| \_ \rightarrow x0 \ (5 \ x1))))
\]

---

**Figure 3.** \( \mu \), optimised according to Theorem 5.

If \( v_1 \) is the value of \( e_1 \), we know that \( v_1 \) necessarily has the
shape \( \text{Def} w \) for some \( w \), because \( e_1 \) contains no spontaneous
divergence and therefore the result cannot be \( \text{Undef} \). Therefore
the result of evaluation of \( e \) is the result of evaluation of \( e_2 \)
in the environment \( (x, \text{Def} w) \rightarrow \rho \). We call this value \( v_2 \). By
induction hypothesis on evaluation of \( e_1 \), we have that the result
of evaluation of \( e_1 \downarrow \) is \( v_1 \downarrow = (\text{Def} w) \downarrow = w \downarrow \). Hence
the result of evaluation of \( e_1 \downarrow \) is the result of evaluation of \( e_2 \downarrow \)
in \( (x, w) \downarrow \rightarrow \rho \downarrow = ((x, \text{Def} w) \rightarrow \rho) \downarrow \). By induction hypothesis,
this evaluation yields \( v_2 \downarrow \).

A model of this proof was formally verified using the Mini-ML
description of the language. This proof is available in \([1]\).

The extracted code of the \( \mu \) function can be optimised accord-
ing to Theorem 5 as shown in Figure 3. Thus we have eliminated
the type partial from the code. Occurrences of \text{Obj} \text{.} \text{magic} still remain
as traces of coercions that appear in the Coq code for \( \mu \). All
these occurrences can be safely erased from the code.

7. **Automation of the Least Fixed Point Definition**

We develop a command we called \text{Fcpo} Function that allows to
define least fixed points of partial recursive functions and automate
certain routine steps in this process. The definition of \( \mu \) using
the new command (in its current version) is the following:

Variable \( A : \text{Type} \).

Variable \( f : A \rightarrow \text{nat} \rightarrow \text{partial} \text{.} \text{nat} \).

\text{Fcpo Function } \mu : A \rightarrow \text{nat} \rightarrow \text{partial} \text{.} \text{nat} := \)

\[
\text{fun } x \ y \Rightarrow
\text{match } f x y \text{ with }
| \text{Undef} \Rightarrow \text{Undef}
| \text{Def } 0 \Rightarrow \text{Def} y
| \_ \Rightarrow \mu x \ (5 \ y)
\text{end.}
\]

Then the command generates the recursive functional \( f \mu \), as in
Section 5 and two proof obligations that the user is required to
satisfy in order to complete the definition:

1. The first obligation is the monotonicity proof for \( f \mu \), fol-
   lowed by the automated definition of the monotonic version of
   \( f \mu \), that is \( \text{mono} \mu \) (see Section 5).

2. The second obligation is the continuity proof for \( \text{mono} \mu \), fol-
   lowed by the definition of the continuous version of \( \text{mono} \mu \),
   that is \( \text{cont} \mu \).

Finally, the required least fixed point of \( \text{cont} \mu \) is defined auto-
matically as \( \text{fixp} \ \text{cont} \mu \).
The syntax of \texttt{Fcpo Function} is the following:

\texttt{Fcpo Function ident [\text{binders}] := terms}:

where \text{term} is a type with target partial \text{A}, for \text{A} a type.

This command is compatible with the standard Coq extraction procedure augmented by the two extraction constants, as we described in Section 4.

8. Future Work

There are a few features related to \texttt{Fcpo Function} that are now in an early development stage:

1. Comprehensive automation of monotonicity and continuity proofs.
2. Automated elimination of the ecpo structure (and hence occurrences of \text{Obj}\text{magic}) from the extracted code.
3. Techniques that allow to hide partial from the user of the command.

In fact, hiding techniques would require full proof automation as well since otherwise one would still need to work at the level of partial types during the work on proof obligations generated by the command.

Our effort to formalise optimisations of the extracted code should also be compared with efforts done to give a formal description of the extraction procedure, as studied by Letouzey \cite{19} and Glonn \cite{15}.

9. Related Work

The work described here contributes to all the work that was done to ease the description and formal proofs about general recursive functions. A lot of effort was put into providing relevant collections of inductive types with terminating computation derived from the notion of primitive recursion \cite{10, 25, 2}. In particular, it was shown that the notion of accessibility or noetherian induction could be described using an inductive predicate in \cite{14}. This accessibility predicate makes it possible to encode well-founded recursion when one can prove that all elements of the input type satisfy the accessibility predicate for a well-chosen relation (such a relation is called well-founded). If it is not true that all elements are accessible (or if one cannot exhibit a well-founded relation that suits the function being defined), the recursive function may still be defined but have well-defined values only for the elements that can be proved to be accessible. This idea was further refined in \cite{14, 15}, where termination is not described using an accessibility predicate, but directly with an inductive predicate that actually describes exactly those inputs for which the function terminates. As a result, formal developers still need to prove that a potentially non-terminating function is only used for inputs for which termination is guaranteed and extracted programs inherit the termination guarantee. By contrast, the approach of this paper relieves the developer from the burden of proving termination and does not guarantee it either, which can be useful for some applications, like interpreters for Turing-complete languages (where termination is undecidable) or functions for which potential non-termination is an accepted defect.

There are analogous techniques that also do not require a termination proof. One such method is Prop-bounded recursion based on a coinductive monad \cite{20}. In this method the coinductive type permits to represent infinitely long computations as (potentially) infinitely large objects of coinductive types. One is also able to write a function that directly refers to itself, which would be incompatible with, e.g., Fixpoint due to syntactic restrictions. However, the coinductive methods require a more complex notion of equality due to the presence of infinite objects, such as, in the case of \cite{21}, the John Major equality which relies on the JMeq axiom of Coq.

Another work \cite{4, 6} attempts to provide tools that stay closer to the level of expertise of programmers in conventional functional programming. The key point is to start from the recursive equation and to generate the recursive function definition from this equation. Users still need to prove that the recursive calls happen on predecessors of the initial input for a chosen well-founded relation, but these requirements appear as proof obligations that are generated as a complement of the recursive equation. The tool produces the recursive function and a proof of the recursive equation. Again, this approach is restricted to total functions. Following this work as an inspiration there was provided a more general command Function \cite{13} that supports several ways of defining recursive functions and related objects such as induction principles.

In one of our experiments \cite{9}, we defined the semantics of a small programming language in the spirit of \cite{14, 13}. We used the Knaster–Tarski fixed point theorem to describe the semantics of while loops as suggested in \cite{20}. Then we were able to prove that when a value is returned, the same computation can be modelled by a natural semantics derivation, using an encoding of the natural semantics based on an inductive predicate. This reproduces a similar formalised proof in \cite{14}. Once extracted to ML, this gives a certified interpreter for the language.

In an early version of the Calculus of Constructions, formalisations of the Knaster–Tarski least fixed point theorem were also used to show how inductive definitions could be encoded directly in the pure (impredicative) Calculus of Constructions \cite{17}. In this respect, it is also worthwhile to mention that \cite{14} shows how this theorem can be used to give a definitional justication of inductive types in higher-order logic.

In this paper, we formalised only the minimal amount of domain theory just enough to make it possible to define simple potentially non-terminating functions and perform basic reasoning steps on these functions. More complete studies of domain theory were performed in the LCF system \cite{28}. It was also formalised in Isabelle’s HOL instantiation to provide a package named as HOLCF \cite{9, 13}. We believe these other experiments can give us guidelines for improvements.

10. Conclusion

There is a popular belief that type-theory based proof tools can only be used to reason about functions that are total and terminating for all inputs, because termination of reductions is needed to ensure the consistency of the systems in question. The major aim of this paper is to provide yet another way to model potentially non-terminating functions. Our inspiration comes from the Knaster–Tarski least fixed point theorem.

Our contributions can be summarised as follows.

First, we formalised a domain theory based on the notion of a preorder and equipped it with flat cpos. This work is analogous to Isabelle/HOLCF and allows one to provide potentially non-terminating functions with a least fixed point semantics in Coq.

Second, we provided arguments in favour of our claim that the fixed point combinator is the right computational value for the Knaster–Tarski theorem and should therefore be used for extraction of functional programs from Coq.

Third, we used two extraction axioms (least fixed point and constructive definite description) in course of extraction and obtained a powerful way to represent in Coq potentially non-terminating functions and reason about them.
Acknowledgments

The authors are grateful to the anonymous referees for their detailed comments. This work has also benefited from suggestions by Benjamin Werner, Hugo Herbelin and Peter Aczel, and also from early experiments by Kuntal Das Barman. The first author also wishes to remember the late Gilles Kahn, who started work on formalized domain theory in the context of the Calculus of Inductive Constructions in mid-90’s [13].

References